Requested Patent: JP11234263A

Title: METHOD AND DEVICE FOR MUTUAL AUTHENTICATION ;

Abstracted Patent: JP11234263 ;

Publication Date: 1999-08-27 ;

Inventor(s): SUZUKI KOJI;; NAKAGAKI JUHEI;; SHIN YOSHIHIRO ;

Applicant(s): FUJI XEROX CO LTD ;

Application Number: JP19980030053 19980212 ;

Priority Number(s): ;

IPC Classification: H04L9/32; G09C1/00; H04L9/10 ;

Equivalents: ;

ABSTRACT:

PROBLEM TO BE SOLVED: To provide a mutual authentication suitable for a device of low arithmetic capacity.SOLUTION: A testifier 101 generates a commitment (w) and sends it to a verifier 111. The verifier 111 sends challenges S, mu and r' to the testifier 101 and calculates an index g=h(r', mu ) for verification while using a unidirectional hash function (h) shared with the testifier 101. The testifier 101 verifies S while using disclosed information, further generates an index g'=h(r', mu ) for verification while using r', mu and (h), generates response generation information y'